(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
21. Juli 2005 (21.07.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/066908 A2

(51) Internationale Patentklassifikation[7]: G08B

(21) Internationales Aktenzeichen: PCT/CH2004/000739

(22) Internationales Anmeldedatum:
16. Dezember 2004 (16.12.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
12/04 6. Januar 2004 (06.01.2004) CH

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **KABA AG** [CH/CH]; Kempten, 8623 Wetzikon (CH).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **STUDERUS, Paul** [CH/CH]; Hüeblistrasse 78, 8165 Oberweningen (CH).

(74) Anwalt: **BREMI, Tobias**; Isler & Peddrazzini AG, Gotthardstrasse 53, Postfach 6940, CH-8023 Zürich (CH).

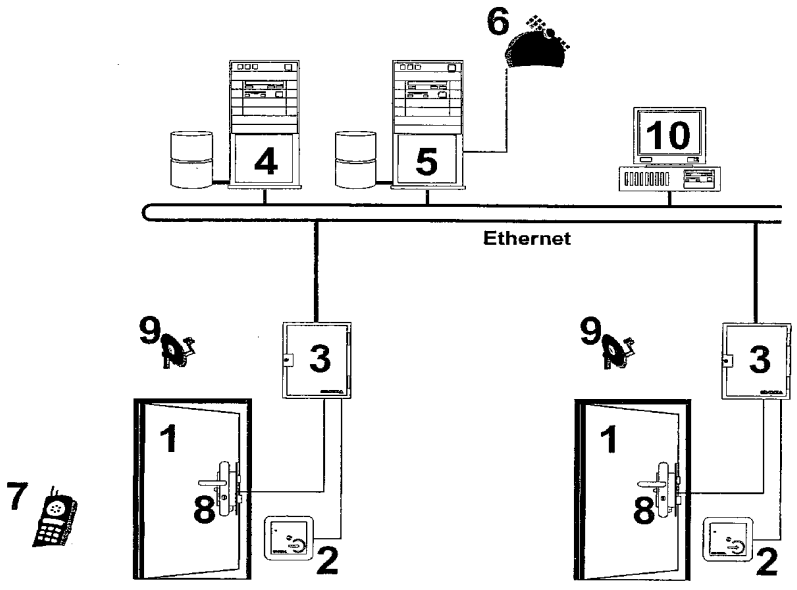
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU,

[Fortsetzung auf der nächsten Seite]

(54) Title: ACCESS CONTROL SYSTEM AND METHOD FOR OPERATING SAID SYSTEM

(54) Bezeichnung: ZUTRITTSKONTROLLSYSTEM UND VERFAHREN ZU DESSEN BETRIEB



(57) Abstract: The invention relates to an access control system and to a method for operating said system. The system uses a standard access control system (2-4, 8), which controls a plurality of access points (1) by means of respective individual physical closing mechanisms (8). According to the invention, at least one reader (2) and a controller (3), which is connected to the latter in order to control the closing mechanism (8), is provided at each access point (1) and the system is equipped with at least one access control server (4), which carries out the centralised management of access data and is connected to the respective controllers (3), in addition to at least one mobile telephone server (5), which is connected to the access control server (4), said mobile telephone server being at least indirectly capable of transmitting data to mobile radio telephone subscribers (7) via a mobile radio telephone network and of receiving data from said subscribers. The mobile radio telephone server (5) can also be an integral component of the access control server (4). The aim of the invention is to provide an access control system that uses mobile telephones, which can be easily retrofitted and is especially user-friendly and at the same time reliable. To achieve this, at least one access point (1) is equipped with a short-range transmitter (9), which transmits identification information that is specific to the access point in such a way that it is only received by a mobile telephone (7) located in the direct vicinity of the access point (1) and is used at least indirectly by said telephone to control the access verification process. The use of Bluetooth or WLAN transmitters (9) is particularly advantageous in this context as modern mobile telephones (7) are already equipped with interfaces of this type and Bluetooth transmitters (9) are cost-effective and readily available.

[Fortsetzung auf der nächsten Seite]

WO 2005/066908 A2

TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

(57) Zusammenfassung: Die vorliegende Erfindung betrifft ein Zutrittskontrollsystem, sowie ein Verfahren zu dessen Betrieb, mit einem Standard-Zutrittskontrollsystem (2-4, 8), über welches eine Vielzahl von Zutrittspunkten (1) über jeweils individuelle physikalische Schliessmnechanismen (8) kontrolliert werden können, wobei bei jedem Zutrittspunkt (1) wenigstens ein Leser (2) sowie ein damit in Verbindung stehender Controller (3) zur Steuerung des Schliessmechanismus' (8) vorgesehen ist, und wobei wenigstens ein Access Control-Server (4) vorhanden ist, welcher eine zentrale Verwaltung der Zutrittsdaten vornimmt, und welcher mit den jeweiligen Controllern (3) in Verbindung steht sowie mit wenigstens einem Mobiltelefonie-Server (5) in Verbindung mit dem Access Control-Server (4), welcher wenigstens indirekt in der Lage ist, Daten über ein Mobiltelefon-Netz an Mobiltelefon-Teilnehmer (7) abzusetzen respektive von diesen zu empfangen, wobei dieser Mobiltelefonie-Server (5) auch integraler Bestandteil des Access Control-Server (4) sein kann. Ein einfach nachrüstbare und besonders benutzerfreundlicher und gleichzeitig sichere Zutrittskontrolle unter Verwendung von Mobiltelefonen wird dabei dadurch gewährleistet, dass bei wenigstens einem Zutrittspunkt (1) ein kurzreichweitiger Sender (9) vorhanden ist, welcher Zutrittspunktspezifische Identifikationsinformation derart aussendet, dass sie von einem nur in unmittelbarer Nähe des Zutrittspunkts (1) befindlichen Mobiltelefon (7) empfangen und von diesem wenigstens indirekt zur Steuerung der Zutrittskontrolle verwendet wird. Insbesondere die Verwendung von Bluetooth- oder WLAN-Sendern (9) erweist sich in diesem Zusammenhang als besonders vorteilhaft, da moderne Mobiltelefone (7) bereits über derartige Schnittstellen verfügen und Bluetooth-Sender (9) kostengünstig und zuverlässig erhältlich sind.

BESCHREIBUNG

TITEL

Zutrittskontrollsystem und Verfahren zu dessen Betrieb

TECHNISCHES GEBIET

Die vorliegende Erfindung betrifft ein Zutrittskontrollsystem, sowie ein Verfahren zu dessen Betrieb. Das Zutrittskontrollsystem basiert auf einem Standard-Zutrittskontrollsystem, über welches eine Vielzahl von Zutrittspunkten über jeweils individuelle physikalische Schliessmechanismen kontrolliert werden können, wobei bei jedem Zutrittspunkt wenigstens ein Leser sowie ein damit in Verbindung stehender Controller zur Steuerung des Schliessmechanismus' vorgesehen ist. Weiterhin ist wenigstens ein Access Control-Server vorhanden, welcher eine zentrale Verwaltung der Zutrittsdaten vornimmt, und welcher mit den jeweiligen Controllern in Verbindung steht, sowie wenigstens ein Mobiltelefonie-Server in Verbindung mit dem Access Control-Server, welcher wenigstens indirekt in der Lage ist, Daten über ein Mobiltelefon-Netz an Mobiltelefon-Teilnehmer abzusetzen respektive von diesen zu empfangen.

STAND DER TECHNIK

Zutrittskontrollsysteme sind im wesentlichen elektronisch gesteuerte zentralisierte

Systeme, welche eine Vielzahl von Zutrittspunkten (Durchgängen) in deren Zugänglichkeit überwachen, steuern und verwalten. Moderne Zutrittskontrollsysteme beruhen dabei häufig auf berührungsloser Technologie, d. h. beim Zutrittspunkt wird nicht mehr ein physikalischer Schlüssel verwendet, sondern elektronisch lesbare Medien, welche durch entsprechende, an den Zutrittspunkten vorgesehene Leser aktiviert und von diesen ausgelesen werden. Diese elektronisch lesbare Medien sind typischerweise unter dem Begriff RFID (Radio Frequency Identification) bekannt und hochstehende Technologien sind beispielsweise bei der Anmelderin unter dem Handelsnamen LEGIC® erfolgreich und zuverlässig seit längerer Zeit in Anwendung.

Bei Verwendung eines RFID Mediums wird im Rahmen eines derartigen Zutrittskontrollsystems normalerweise wie folgt vorgegangen:

Eine Person steht vor dem Leser des Durchganges (Zutrittspunkt), für welchen er Zutritt erlangen möchte. Er präsentiert sein Medium (RFID-Tag) und das System prüft, ob das Medium bekannt ist, ein Profil vorhanden ist und dieses den Zutritt zu diesem Zeitpunkt zulässt. Wenn OK, wird das am Leser signalisiert und die Tür einmalig durch den Controller freigegeben.

Diese Technologie eignet sich insbesondere bei ständigen Mitarbeitern, welche einmal mit einem derartigen elektronischen Medium ausgestattet werden können, welches anschliessend sowohl Zutrittskontrolle, gegebenenfalls zudem Zeiterfassung oder weitere Applikationen, ermöglicht.

In zunehmendem Masse wird es in heutiger Zeit aber erforderlich, auch kurzfristig Zutrittsberechtigungen an Servicepersonal oder Ähnliches zu vergeben, dies gegebenenfalls in Notsituationen auch auf einer sehr kurzen Zeitskala, was die Abgabe von entsprechenden physikalischen Medien (zum Beispiel RFID-Tags) so gut wie verunmöglicht. Zudem beinhaltet jede Abgabe von entsprechenden Medien das Risiko eines Verlustes und damit von Sicherheitslücken.

In neuerer Zeit ist entsprechend die Tendenz und das Bedürfnis aufgekommen, gegebenenfalls Mobiltelefone (Handys) als Ersatz oder zumindest Ergänzung für diese elektronischen Medien zu verwenden. In diesem Fall wird typischerweise wie folgt

vorgegangen:

Eine Person gibt die Durchgangsnummer (d. h. eine Kennung des spezifischen Zutrittspunkts), für welchen er Zutritt erlangen möchte, in einem Handy Dialog ein. Er bestätigt die Eingabe gegebenenfalls mit seinem persönlichen PIN Code. Diese Daten werden über das Mobiltelefon-Netz an den Zutrittssystem Server (Access Control-Server) gesendet. Dort wird geprüft, ob die Handynummer bekannt ist, der PIN Code korrekt ist, ein Profil vorhanden ist (ist diese Handynummer mit diesem PIN Code zu diesem spezifischen Zeitpunkt an diesem spezifischen Zutrittspunkt autorisiert) und dieses den Zutritt zu diesem Zeitpunkt zulässt. Wenn OK, wird das am Leser signalisiert und die Tür einmalig durch den Controller freigegeben (hier ausgelöst durch den Server).

DARSTELLUNG DER ERFINDUNG

Der Erfindung liegt demnach die Aufgabe zugrunde, ein in diesem Zusammenhang verbessertes Zutrittskontrollsystem, sowie ein Verfahren zu dessen Betrieb vorzuschlagen. Das Zutrittskontrollsystem basiert auf einem Standard-Zutrittskontrollsystem, über welches eine Vielzahl von Zutrittspunkten über jeweils individuelle physikalische Schliessmechanismen kontrolliert werden können, wobei bei jedem Zutrittspunkt wenigstens ein Leser sowie ein damit in Verbindung stehender Controller zur Steuerung des Schliessmechanismus' vorgesehen ist. Weiterhin ist wenigstens ein Access Control-Server vorhanden, welcher eine zentrale Verwaltung der Zutrittsdaten vornimmt, und welcher mit den jeweiligen Controllern in Verbindung steht, sowie wenigstens ein Mobiltelefonie-Server in Verbindung mit dem Access Control-Server, welcher wenigstens indirekt in der Lage ist, Daten über ein Mobiltelefon-Netz an Mobiltelefon-Teilnehmer abzusetzen respektive von diesen zu empfangen.

Die Lösung dieser Aufgabe wird dadurch erreicht, dass an einem spezifizierten Ort ein kurzreichweitiger Sender vorhanden ist, welcher Zutrittspunkt-spezifische Identifikationsinformation derart aussendet, dass sie von einem nur in Empfangsnähe

des Senders befindlichen Mobiltelefon empfangen und von diesem wenigstens indirekt zur Steuerung der Zutrittskontrolle eines spezifischen zugeordneten Zutrittspunkts verwendet wird.

Der Kern der Erfindung besteht somit darin, einerseits nur Mobiltelefonen die Öffnung am Zutrittspunkt zu erlauben, welche auch tatsächlich in unmittelbarer Nähe dieses Senders und damit in unmittelbarer Nähe eines spezifischen Orts sind. Andernfalls wäre es nämlich möglich, einen entsprechenden Ablauf mit einem Mobiltelefon auszulösen, ohne physisch vor Ort oder an einem spezifizierten Ort zu sein. Dabei handelt es sich um eine Sicherheitslücke. Im vorliegenden Fall wird dies nun verhindert, indem nur eine entsprechende Öffnungsanfrage durch das Mobiltelefon abgesetzt werden kann, wenn es über eine entsprechende Schnittstelle die Identifikationsinformation des Senders empfängt.

Beim spezifischen Ort kann es sich dabei einerseits um die unmittelbare Nähe des zugeordneten Zutrittspunkts handeln, wobei in diesem Fall die Positionierung des Senders bevorzugt so vorgenommen wird, dass das Mobiltelefon diesen Sender nur empfangen kann, wenn es sich unmittelbar vor dem Zutrittspunkt befindet.

Andererseits ist es aber auch möglich, den Sender bewusst dem Zutrittspunkt vorgelagert anzuordnen, beispielsweise im Falle einer Zufahrt derart, dass ein Lastwagenfahrer ohne auszusteigen mit seinem Mobiltelefon einen Zugang öffnen kann.

Eine grundsätzlich andere Alternative besteht darin, einen bestimmten Bereich zur Autorisierung eines spezifischen Zuganges freizugeben. So kann zum Beispiel ein Sender in einem Überwachungsraum oder einem anderen Arbeitsraum angeordnet werden, so dass Personal, wenn es sich in diesem Überwachungsraum befindet, über ein Mobiltelefon eine oder mehrere Zutrittspunkte öffnen kann. Insbesondere in diesem Fall ist es auch möglich, einem Sender mehrere Zutrittspunkte zuzuordnen. In diesem Fall muss aber anschliessend bei der Autorisierung über den Access Control-Server noch angegeben werden, welcher der der gleichen Identifikation zugeordneten Zutrittspunkte geöffnet werden soll.

Der Empfang der Identifikationsinformation des Senders beinhaltet aber andererseits

auch eine zusätzliche Vereinfachung und Erhöhung der Sicherheit in anderer Hinsicht. Ohne eine entsprechende lokale Kennung muss der Benutzer des Mobiltelefons, sofern er nicht nur zum Zutritt an einem einzigen Zutrittspunkt berechtigt ist, in einem bestimmten Moment eine Kennung des spezifischen Zutrittspunkts an seinem Mobiltelefon eingeben. Dieser Vorgang ist einerseits mühselig und andererseits fehleranfällig sowie manipulierbar. Grundsätzlich käme für eine derartige Lokalisierung auch die Zelleninformation des Mobiltelefons in Frage, es zeigt sich in der Praxis aber, dass einerseits die Zelleninformation normalerweise für individuelle Zutrittspunkte lokal zu wenig genau ist (unterschiedliche Durchgänge in der gleichen Zelle), und dass die von einem spezifischen Benutzer gerade verwendete Zelle auch je nach Mobiltelefon-Betreiber unterschiedlich sein kann und zudem bei verändernden Zellen im Zutrittskontrollsystem stets nachgeführt werden müsste.

Ein weiterer wesentlicher Vorteil des vorgeschlagenen Verfahrens besteht darin, dass eigentlich nicht das Mobiltelefon als so genanntes "trusted device" verwendet wird, sondern dass nur die einem Mobiltelefon zugeordnete Telefonnummer, wie sie von Access Control-Server respektive vom zugehörigen Mobiltelefonie-Server empfangen wird, zur Authentifikation, gegebenenfalls in Kombination mit einem PIN-Code verwendet wird. Es werden mit anderen Worten keine spezifischen Daten auf dem Mobiltelefon abgelegt, und es ist gegebenenfalls möglich, beispielsweise solange die gleiche SIM-Karte verwendet wird, auch ein anderes Mobiltelefon für die gleichen Zutrittsberechtigungen zu verwenden.

In diesem Zusammenhang muss noch erwähnt werden, dass unter dem Begriff Mobiltelefon grundsätzlich Geräte zu verstehen sind, welche einerseits in der Lage sind, über ein mobiles Telefonnetz, beispielsweise das GSM-Netz, Daten mit dem Access-Control-System auszutauschen, und welche andererseits dazu in der Lage sind, die vom Sender ausgestrahlten Signale zu empfangen, d. h. welche über eine entsprechende Schnittstelle verfügen. Es muss sich entsprechend nicht zwingend um ein Mobiltelefon im klassischen Sinne handeln, es kann sich auch um einen PDA (Personal Digital Assistant) oder einen anderen Computer handeln, solange er über die genannten Möglichkeiten der Kommunikation mit dem Sender respektive dem Zutrittskontroll-

System verfügt.

Gemäss einer ersten bevorzugten Ausführungsform der vorliegenden Erfindung handelt es sich beim Sender um ein Bluetooth-Gerät, insbesondere bevorzugt mit einer Reichweite von weniger als 10 Metern. Moderne Mobiltelefone verfügen normalerweise über Bluetooth-Schnittstellen, und entsprechend erweist es sich als besonders einfach, da keine zusätzliche benutzerseitige Hardware erforderlich ist, die jeweiligen Sender am Zutrittspunkt als Bluetooth-Gerät auszugestalten. Der Bluetooth-Standard führt in automatisierter Weise eine ständige Abfrage und einen ständigen Empfang von den einzelnen Geräten spezifisch zugeordneten, 48-Bit-Adressen durch. Kommt ein solches Mobiltelefon somit in den Bereich eines anderen Bluetooth Gerätes, so wechseln sie gegenseitig automatisch die ID (48-Bit Adresse) aus. Diese Tatsache wird gemäss der Erfindung zur "Lokalisierung" ausgenutzt. Am betroffenen Durchgang (Zutrittspunkt) wird einfach ein Bluetooth Gerät angeordnet. Die ID dieses Gerätes wird im System dem Leser respektive dem Zutrittspunkt zugewiesen. Es handelt sich somit vorzugsweise bei der Identifikationsinformation um eine Hardware-spezifische, eindeutige Adresse des Senders, insbesondere bevorzugt um eine gerätespezifische 48-bit-Adresse eines Bluetooth-Geräts.

Eine Alternative oder zusätzliche Möglichkeit besteht darin, einen WLAN-Sender (Wireless Local Area Network, kurz WLAN, auch wi-fi, steht für "drahtloses lokales Netzwerk", wobei meistens der Standard IEEE 802.11 gemeint ist. Dieser Standard spezifiziert mehrere drahtlose Übertragungstechniken und Verfahren zum Mediumzugriff. Geräte, die nach der Variante 802.11b arbeiten, übertragen Daten per Radiowellen im lizenzfreien ISM-Band bei 2,4 GHz mit einer Brutto-Übertragungsrate von bis zu 11 MBit/s) zu verwenden. Vorteilhaft ist diese Lösung insbesondere deshalb, weil derartige WLAN-Geräte gegebenenfalls in einem Gebäude bereits vorhanden sind, und weil zunehmend insbesondere PDAs überentsprechende Schnittstellen verfügen.

Will jetzt eine Person Zutritt mit einem Mobiltelefon erlangen, muss dieses im Bereich jenes Bluetooth/WLAN Senders sein, welcher dem Durchgang zugewiesen ist. Dies kann physikalisch am gleichen, aber auch an unterschiedlichem Ort verglichen mit dem Leser sein (z.B. Lastwagenzufahrt oder Überwachungsraum). Damit erübrigt sich auch

die Eingabe der Durchgangsnummer (über Bluetooth ID resp. WLAN-Kennung automatisch bekannt, bei der Installation des Bluetooth/WLAN-Gerätes am Zutrittspunkt muss dem System nur einmal die entsprechende Korrelation zwischen Bluetooth/WLAN ID und Zutrittspunkt angegeben werden). Gegebenenfalls mit einem PIN oder einer anderen Authentifikation wird jetzt diese ID an den Zutrittskontroll-Server gesandt. Im Gegensatz zu bereits bekannten Systemen der Zutrittskontrolle unter Verwendung von Bluetooth-Technologie wird im vorliegenden Fall aber nicht eine effektive Verbindung zwischen dem Mobiltelefon und dem Bluetooth-Gerät am Zutrittspunkt hergestellt, sondern es wird am Zutrittspunkt vom Mobiltelefon nur die ID des Bluetooth-Gerätes ausgelesen, um diese Information anschliessend zur Lokalisierung des Mobiltelefons zu verwenden. Die eigentlich möglichen Übermittlungsfunktionen der Bluetooth- resp. WLAN Schnittstelle werden mit anderen Worten nicht verwendet. Dies unter anderem, da die alleinige Verwendung der Bluetooth-Schnittstelle eine vollständige Integration des Bluetooth-Gerätes am entsprechenden Zutrittspunkt erforderlich und dabei ein Nachrüsten aufwändig macht. Im vorliegenden Fall ist nämlich ein wesentlicher Punkt darin zu sehen, dass ein Standard-Zutrittskontrollsystem in besonders einfacher Weise nachgerüstet werden kann.

Der Sender kann im vorliegenden Fall als unabhängige, auch mit einer individuellen Stromversorgung ausgestattete Einheit ausgebildet werden, da er gewissermassen nur zur Erzeugung der Lokalisierungsinformation auf dem Mobiltelefon dient. Der Sender, wie gesagt bevorzugt ein Bluetooth- oder ein WLAN Gerät, verfügt somit bevorzugt über keine direkte Verbindung mit dem Standard-Zutrittskontrollsystem und/oder dem Mobiltelefonie-Server. Ausserdem kann die Übermittlung einer ID auf einer sehr kurzen Zeitskala von weniger als ein paar Sekunden erfolgen, während typischerweise der Aufbau einer effektiven Bluetooth-Verbindung im Bereich von 10 Sekunden dauert. Dies ist in der Regel eine in der Praxis zu lange Zeitspanne. Es wird somit nur ein sehr spezifischer Aspekt der Bluetooth-Technologie verwendet, welcher gewissermassen die Vorteile im Zusammenhang mit Zutrittskontrolle aufgreift, ohne die Nachteile wie beispielsweise langsamer Verbindungsaufbau in Kauf nehmen zu müssen.

Vorzugsweise handelt es sich um ein Zutrittskontrollsystem, welches hauptsächlich Zutrittskontrolle unter Verwendung von Standard-Technologie verwaltet. Das Standard Zutrittskontrollsystem erlaubt somit in der Hauptsache beispielsweise die Zutrittskontrolle unter Verwendung von Mitteln ohne Mobiltelefonie, insbesondere auf Basis von RFID-Technologie.

Für Notfallsituationen ist es gegebenenfalls vorteilhaft, den Sender derart auszugestalten, dass der Sender zusätzlich über eine Verbindung mit dem Controller verfügt, so dass für den Fall eines Ausfalls der Verbindung zwischen Controller und Access Control-Server benutzerspezifische Identifikationsinformation vom Mobiltelefon an den Sender übermittelt und von diesem zur Steuerung des Schliessmechanismus an den Controller übergeben werden kann. Während mit anderen Worten beim normalen Betrieb der Sender ausschliesslich als Sender wirkt, und somit Information nur vom Sender an das Mobiltelefon übermittelt wird, kann in Notfallsituationen auch zusätzlich der umgekehrte Weg freigegeben werden, d. h. es ist möglich, vom Mobiltelefon Information an den Sender, welcher dann als Empfänger wirkt, zu übergeben.

Weiterhin betrifft die vorliegende Erfindung ein Verfahren zur Zutrittskontrolle, insbesondere bevorzugt unter Verwendung eines Zutrittskontrollsystems, wie es oben beschrieben wurde. Dabei ist ein Standard-Zutrittskontrollsystem vorhanden, über welches eine Vielzahl von Zutrittspunkten über jeweils individuelle physikalische Schliessmechanismen kontrolliert werden können, wobei bei jedem Zutrittspunkt bevorzugt wenigstens ein Leser sowie ein damit in Verbindung stehender Controller zur Steuerung des Schliessmechanismus' vorgesehen ist. Ausserdem ist wenigstens ein Access Control-Server vorhanden, welcher eine zentrale Verwaltung der Zutrittsdaten vornimmt, und welcher mit den jeweiligen Controllern in Verbindung steht. Weiterhin ist wenigstens ein Mobiltelefonie-Server in Verbindung mit dem Access Control-Server vorhanden, welcher wenigstens indirekt in der Lage ist, Daten über ein Mobiltelefon-Netz an Mobiltelefon-Teilnehmer abzusetzen respektive von diesen zu empfangen, wobei dieser Mobiltelefonie-Server auch integraler Bestandteil des Access Control-Servers sein kann. Zudem ist bei wenigstens einem Zutrittspunkt oder allgemeiner an

einem spezifischen Ort ein kurzreichweitiger Sender angeordnet.

Erfindungsgemäss wird nun so vorgegangen, dass ein Mobiltelefon zum Zutritt bestimmter Zutrittspunkte in einem bestimmten Zeitraum über den Access Control-Server respektive über den Mobiltelefonie-Server über das Mobiltelefon-Netz autorisiert wird. Dieser Vorgang kann von entsprechendem Personal ausgelöst werden. Der Sender beim entsprechenden Zutrittspunkt oder allgemeiner am spezifischen Ort sendet Zutrittspunkt-spezifische Identifikationsinformation kontinuierlich oder abschnittsweise derart aus, dass sie von einem nur in unmittelbarer Nähe des Zutrittspunkts (wenn der Sender in dessen Nähe angeordnet ist) respektive des Senders befindlichen Mobiltelefon empfangen werden kann (Kontrolle der physischen Präsenz am Zutrittspunkt resp. beim Sender). Ein in unmittelbarer Nähe des Zutrittspunkts resp. des Senders befindliches Mobiltelefon erfasst nun die Kennung dieses Zutrittspunkts über diese Identifikationsinformation, und anschliessend wird automatisiert über Mobiltelefon, Mobiltelefon-Netz, Mobiltelefonie-Server, Access Control-Server, respektive Controller die Öffnung des entsprechenden Zutrittspunktes unter direkter oder indirekter Verwendung dieser Identifikationsinformation veranlasst. Die Übermittlung der Daten schied dabei um Mobiltelefon bevorzugt über das Mobiltelefon-Netz entweder als telefonische Übermittlung oder als Email oder als SMS (Short Message Service, Kurznachrichten-Dienst, CEPT-Standard für kurze Text-Nachrichten, d.h. bis zu 160 alphanumerische Zeichen, an Mobiltelefone im GSM-Netz, die auf dem Handy-Display dargestellt werden).

Gemäss einer ersten bevorzugten Ausführungsform verlangt das Mobiltelefon nach Erfassung der Identifikationsinformation zusätzlich die Eingabe einer Authentifikation wie insbesondere eines PIN-Codes, Passworts, biometrischer Information, und diese benutzerspezifische Information wird anschliessend zusammen mit der Kennung des zu bearbeitenden Zutrittspunkts über das Mobiltelefon-Netz an den Mobiltelefonie-Server und den Access Control-Server übergeben. Anschliessend wird bei entsprechender Berechtigung der zugehörige Controller aktiviert respektive der Schliessmechanismus ausgelöst.

Wie bereits weiter oben erwähnt, handelt es sich beim Sender vorzugsweise um ein

Bluetooth- oder ein WLAN-Gerät, welches als Identifikationsinformation seine eindeutige 48-Bit-Adresse aussendet. Diese 48-Bit-Adresse dient zur Kennung des zugehörigen Zutrittspunkts. Das Mobiltelefon verfügt über eine Bluetooth-Schnittstelle, wobei das Mobiltelefon bei Empfangen spezifischer, im Rahmen der Autorisierung übertragener derartiger 48-Bit-Adressen, welche den autorisierten Zutrittspunkten entsprechen, d. h. von diesem erkannt werden, automatisch in einen entsprechenden Dialog mit dem Mobiltelefon-Benutzer eintritt. Gegebenenfalls wird anschliessend eine Authentifikation des Benutzers angefordert (z. B. PIN-Code). Auf jeden Fall wird anschliessend eine Öffnungsanfrage des spezifischen Zutrittspunkts über das Mobiltelefon-Netz an den Mobiltelefonie-Server respektive den Access Control-Server übermittelt. Nach Überprüfung der Berechtigung wird anschliessend der Access Control-Server, sofern die Berechtigung gegeben ist, eine Auslösung des Controllers vornehmen.

Die Sicherheit lässt sich weiterhin verbessern, wenn gemäss einer weiteren bevorzugten Ausführungsform des erfindungsgemässen Verfahrens das Bluetooth- resp. WLAN-Gerät derart im Bereich des Zutrittspunktes angeordnet, dass der Empfang der Identifikationsinformation durch ein Mobiltelefon nur in einem Abstand von weniger als 1m, bevorzugt weniger als 0.5m ausserhalb und vor dem Zutrittspunkt möglich ist.

Weitere bevorzugte Ausführungsformen des Zutrittskontrollsystems respektive des Verfahrens zur Zutrittskontrolle sind in den abhängigen Ansprüchen beschrieben.

Weiterhin betrifft die vorliegende Erfindung ein Zeiterfassungssystem, welches ebenfalls auf der identischen Idee beruht, einen Sender, insbesondere ein Bluetooth-Gerät ausschliesslich dazu zu verwenden, die physische Anwesenheit eines Mobiltelefons zur Öffnung von Datentransfer zu kontrollieren. Das Zeiterfassungssystem verfügt dabei über ein Standard-Zeiterfassungssystem, welches wenigstens einen Zeiterfassungs-Server umfasst, welcher eine zentrale Verwaltung der Zeitdaten vornimmt; es verfügt weiterhin über wenigstens einen Mobiltelefonie-Server in Verbindung mit dem Zeiterfassungs-Server, welcher wenigstens indirekt in der Lage ist, Daten über ein Mobiltelefon-Netz an Mobiltelefon-Teilnehmer abzusetzen respektive von diesen zu empfangen, wobei dieser Mobiltelefonie-Server auch

integraler Bestandteil des Zeiterfassungs-Servers sein kann. Das Zeiterfassungssystem zeichnet sich erfindungsgemäss dadurch aus, dass bei wenigstens einem autorisierten Bereich ein kurzreichweitiger Sender vorhanden ist, welcher Bereichs-spezifische Identifikationsinformation derart aussendet, dass sie nur von einem in unmittelbarer Nähe des autorisierten Bereichs befindlichen Mobiltelefon empfangen und von diesem wenigstens indirekt zur Manipulation der Zeitdaten verwendet wird. Auf diese Weise kann sichergestellt werden, dass bei Verwendung von Mobiltelefonen zur Zeiterfassung entsprechende Anfragen respektive Eingaben nur in spezifischen Bereichen ermöglicht sind. So können beispielsweise einzelne Stockwerke oder nur Eingangsbereiche etc. autorisiert werden, was einem Missbrauch vorbeugt.

Weiterhin betrifft die vorliegende Erfindung ein Verfahren zur Zeiterfassung, insbesondere bevorzugt unter Verwendung eines Zeiterfassungssystems, wie es oben beschrieben wurde. Das Verfahren umfasst dabei ein Standard-Zeiterfassungssystem, mit wenigstens einem Zeiterfassungs-Server, welcher eine zentrale Verwaltung der Zeitdaten vornimmt; weiterhin ist wenigstens ein Mobiltelefonie-Server in Verbindung mit dem Zeiterfassungs-Server vorhanden, welcher wenigstens indirekt in der Lage ist, Daten über ein Mobiltelefon-Netz an Mobiltelefon-Teilnehmer abzusetzen respektive von diesen zu empfangen, wobei dieser Mobiltelefonie-Server auch integraler Bestandteil des Zeiterfassungs-Servers sein kann; ausserdem ist bei wenigstens einem autorisierten Bereich ein kurzreichweitiger Sender vorhanden.

Das Verfahren ist nun insbesondere dadurch gekennzeichnet, dass ein Mobiltelefon zur Eingabe von Zeitdaten in bestimmten autorisierten Bereichen in wenigstens einem bestimmten Zeitraum über den Zeiterfassungs-Server respektive über den Mobiltelefonie-Server über das Mobiltelefon-Netz autorisiert wird, dass der Sender Bereichs-spezifische Identifikationsinformation kontinuierlich oder abschnittsweise derart aussendet, dass sie nur von einem in unmittelbarer Nähe des autorisierten Bereichs befindlichen Mobiltelefon empfangen werden kann, dass ein in unmittelbarer Nähe des Bereichs befindliches Mobiltelefon die Kennung dieses Bereichs über diese Identifikationsinformation erfasst, und dass anschliessend über Mobiltelefon, Mobiltelefon-Netz, Mobiltelefonie-Server Zeitdaten an den Zeiterfassungs-Server

übermittelt, respektive von diesem abgefragt werden können.

Weitere bevorzugte Ausführungsformen des Zeiterfassungssystems respektive des Verfahrens zur Zeiterfassung sind in den abhängigen Ansprüchen beschrieben.

Nicht zuletzt betrifft die vorliegende Erfindung ausserdem ein spezifisches Datenverarbeitungsprogramm (Software), welches auf einem Mobiltelefon lauffähig ist, und welches die Durchführung eines Verfahrens zur Zutrittskontrolle respektive zur Zeiterfassung, wie es oben beschrieben wurde, zu implementieren erlaubt. Das Datenverarbeitungsprogramm ist dazu in der Lage, in automatisierter Weise die vom Sender empfangene Identifikationsinformation, gegebenenfalls in Kombination mit einer weiteren Identifikation wie beispielsweise PIN-Code oder Ähnliches, an die Zutrittskontrolle zu übermitteln. Weiterhin betrifft die vorliegende Erfindung ein Mobiltelefon oder grundsätzlich ein anderes Gerät, auf welchem ein derartiges Datenverarbeitungsprogramm geladen ist, oder von welchem ein derartiges Datenverarbeitungsprogramm heruntergeladen werden kann.

KURZE ERLÄUTERUNG DER FIGUR

Die Erfindung soll nachfolgend anhand von Ausführungsbeispielen im Zusammenhang mit der Zeichnung näher erläutert werden. Fig. 1 zeigt eine schematische Darstellung eines Zutrittskontrollsystems.

WEGE ZUR AUSFÜHRUNG DER ERFINDUNG

Fig. 1 zeigt in schematischer Darstellung ein Zutrittskontrollsystem. Anhand dieser Darstellung soll die Erfindung erläutert werden, ohne dadurch die Breite des Schutzes, wie er in den Ansprüchen formuliert ist, einzuschränken.

Das Zutrittskontrollsystem umfasst einen Access Control-Server 4, auf welchem die Zutrittsberechtigungen festgelegt und verwaltet werden. Der Access Control-Server 4 kann neben Zutrittskontrolle auch gleichzeitig Zeitkontrolle übernehmen, d. h. die entsprechenden Zeitdaten personenspezifisch ablegen und verwalten. Der Access

Control-Server 4 ist einerseits mit einer Vielzahl von Zutrittspunkten, d. h. Durchgänge 1 respektive 1' verbunden. Er verwaltet den Zutritt, d. h. die mögliche Öffnung und/oder Schliessung dieser Zutrittspunkte. An den einzelnen Zutrittspunkten 1 ist dazu zunächst ein Controller 3 angeordnet, welcher u.a. als Interface zum Access Control-Server 4 dient, und auf welchem je nach Ausgestaltung des Systems gewisse Informationen des Access Control-Servers gespiegelt sind. Die Controller 3 übernehmen einerseits die Aufgabe, die von einem Leser 3 empfangenen Daten zu verarbeiten, und diese entweder direkt oder erst nach entsprechender Rücksprache der Zutrittsberechtigungen auf dem Access Control-Server 4 zu benutzen. Benutzen heisst hier, dass der Controller 3 entsprechende Schliessmechanismen 8 physikalisch aktiviert, d. h. beispielsweise Riegel zurückführt oder Ähnliches, so dass der Zutrittspunkt, d. h. der Durchgang 1 vom Benutzer geöffnet werden kann.

Beim bis zu diesem Punkt geschilderten Zutrittskontrollsystem handelt es sich um ein Zutrittskontrollsystem nach dem Stand der Technik. Derartige Zutrittskontrollsysteme können dabei in Kombination mit elektronischen, mechatronischen und/oder mechanischen Komponenten verwendet werden, und sind beispielsweise von der Anmelderin unter dem Handelsnamen Kaba exos® in Kombination mit RFID-Technologien unter dem Namen LEGIC® erhältlich.

Es soll nun davon ausgegangen werden, dass ein derartiges Zutrittskontrollsystem unter Verwendung von RFID-Technologie bereits vorliegt, d. h. die Leser 2 sind darauf ausgelegt, entsprechende RFID-Tags auszulesen. Ein derartiges System soll nun für spezifische Situationen in einfacher Weise nachgerüstet werden, so dass Personen, welche normalerweise in derartig verwalteten Gebäuden nicht zutrittsberechtigt sind, d. h. welche nicht bereits über ein entsprechendes RFID-Gerät verfügen, insbesondere kurz- oder mittelfristig zutrittsberechtigt werden sollen. Zunächst wird dazu eine Möglichkeit vorgesehen, die Zutrittsberechtigungen über Mobiltelefone 7 zu ermöglichen. Dazu muss das Zutrittskontrollsystem zunächst an das Mobiltelefon-Netz angebunden werden. Zu diesem Zweck wird an den Access Control-Server 4 ein GSM-Server 5 (Global System for Mobile Communication) angebunden. Dieser GSM-Server 5 steht wenigstens indirekt mit einer Antenne 6 in Verbindung, welche es erlaubt, mit

Mobiltelefonen 7, typischerweise über Relaisstationen etc., zu kommunizieren.

Weiterhin ist an jedem Zutrittspunkt 1 ein Bluetooth oder alternativ resp. zusätzlich Wireless LAN (WLAN)-Gerät 9 angeordnet. Dieses Gerät 9 ist dabei im Bereich des Zutrittspunktes 1 derart vorgesehen, dass ein korrespondierender Empfänger, beispielsweise ein Mobiltelefon 7 mit einer Bluetooth oder WLAN-Schnittstelle, dieses Gerät 9 nur dann empfängt, wenn das Mobiltelefon 7 im wesentlichen unmittelbar vor dem Durchgang 1 angeordnet ist.

Bluetooth ist grundsätzlich ein Protokoll für drahtlose (wireless) Datenübertragung. Der Standard dient zur Datenübertragung durch kurzwelligen Funk im global lizenzfrei nutzbaren ISM-Netz (2.45 GHz, wie in IEEE 802.11b) bei einer Reichweite von maximal 10 m, durch Verstärkung bis zu maximal 100m (im vorliegenden Fall in der Regel nicht vorgesehen). Die Übertragungsgeschwindigkeit erreicht 1MBit/s. Der Verbindungstyp ist one-to-one. Ausser einem Datenkanal stehen auch Sprachkanäle zur Verfügung. Vorgesehen ist dieses System insbesondere für so genannte PANs (Personal Area Network), d. h. für sehr lokale persönliche kabellose Netzwerke, welche möglichst automatisch, d. h. ohne spezifische Einflussnahme des Benutzers, aufgebaut werden sollen. Gemeint ist somit der Nahbereich von maximal zehn Metern um eine Person.

Durch das Bluetooth Verfahren soll die kabelgebundene Datenübertragung überflüssig werden. Dadurch lassen sich etwa kabellose Local Area Networks installieren, oder die Datenübertragung zwischen mobilen und stationären Geräten ermöglichen. Dabei kann der Datenaustausch auch automatisch erfolgen, sobald die Reichweite unterschritten wird. Ein weiterer Anwendungsbereich ist die Vernetzung im Privatbereich.

Um Bluetooth-fähig zu sein, müssen die Geräte mit einem Bluetooth-Chip zur Sende- und Empfangssteuerung ausgestattet sein. Der Bluetoothstandard wurde von der Bluetooth Special Interest Group spezifiziert, Bluetooth 1.0 im Juli 1999. Der Standard ist offen. Jedes Gerät verfügt über eine eindeutige 48-Bit Adresse, welche ständig nach aussen kommuniziert wird. Kommen zwei Bluetooth-fähige Geräte in genügend nahen Kontakt, so tauschen sie gem. Protokoll automatisch die korrespondierenden ID-Adressen aus.

Wireless LAN (WLAN) ist ein weiterer, offener Standard (IEEE 802.11) für drahtlose Datenübertragung und wird im Gegensatz zu Bluetooth vor allem bei grösseren Datenmengen und Distanzen in Zukunft vermehrt Verwendung finden. Auch hier wird mit drahtloser Datenübermittlung und einer jeweils eindeutigen Kennung gearbeitet und das WLAN eignet sich somit ebenfalls für das vorgeschlagene Verfahren. Dies insbesondere, da zunehmend mobiltelephoniefähige Geräte mit WLAN-Schnittstellen ausgerüstet werden (z.B. mobiltelephoniefähige PDAs). Stehen keine Mobiltelefone mit Bluetooth zur Verfügung, oder muss eine grössere Reichweite möglich sein, oder ist z.B. eine derartige WLAN Ausrüstung in einem Gebäude bereits vorhanden, kann alternativ oder parallel auch diese Technologie im vorgeschlagenen Verfahren zur Anwendung kommen. Grundsätzlich bietet somit der Bluetooth oder der WLAN-Standard eine sehr breite Palette an Kommunikationsmöglichkeiten an. Im vorliegenden Fall wird das Bluetooth/WLAN-Gerät 9 aber nur dazu verwendet, als Sender zu dienen, d. h. es wird nur die Eigenschaft ausgenützt, dass ein derartiges Gerät 9 ständig seine eindeutige Adresse aussendet. Dies, um wie bereits erwähnt, die physikalische Präsenz des Mobiltelefons im Bereich des Zutrittspunktes 1 sicherzustellen und um die Identität des Zutrittspunktes zu übermitteln.

Die Nachrüstung des konventionellen Zutrittskontrollsystems mit derartigen Bluetooth oder WLAN-Geräten 9 ist äusserst einfach. Im wesentlichen besteht sie darin, bei jedem gegebenenfalls freizugebenden Eingang ein derartiges Gerät 9 derart anzubringen, dass ein Empfang durch ein Mobiltelefon 7 im wesentlichen nur unmittelbar vor dem Eingang 1 möglich ist. Typischerweise sollte ein Empfang der spezifischen ID des Gerätes 9 durch ein Mobiltelefon 7 nur möglich sein, wenn das Mobiltelefon 7 näher als einen Meter vor dem Eingang 1 ist.

Insbesondere vorteilhaft an der vorliegenden Erfindung ist es, dass das Gerät 9 in keiner Weise physikalisch in das Zutrittskontrollsystem eingebunden werden muss, d. h. es ist nicht erforderlich, das Gerät 9 beispielsweise an den Controller 3 anzuschliessen und mit diesem zu koordinieren. Das Gerät 9 wird nur im Bereich des Durchgangs 1 angeordnet und kann beispielsweise zudem über eine separate Stromversorgung versorgt werden. Der einzige Schritt, welcher anschliessend erforderlich ist, ist eine

Zuordnung der eindeutigen Adresse eines spezifischen Gerätes 9 zu einem spezifischen Durchgang 1. Dazu reicht es, diese ID einmal auszulesen, und anschliessend im Access Control-Server 4 dem spezifischen Eingang 1 diese ID zuzuordnen. So wird gewissermassen ein virtueller Zutrittspunkt geschaffen.

Im folgenden soll nun ein beispielhaftes Verfahren beschrieben werden, in welchem eine temporäre Zutrittskontrolle vergeben wird:

Im Rahmen von Unterhaltsarbeiten in einem Gebäude, welches mit einer Zutrittskontrolle verwaltet wird, soll einer Person ausnahmsweise für einen Nachmittag die Berechtigung vergeben werden, jeweils den Haupteingang eines Gebäudekomplexes zum Zugang benutzen zu können.

Ein Verwalter des Zutrittskontrollsystems gibt anschliessend direkt oder indirekt auf dem Access Control-Server 4 anstelle oder zusätzlich zum RFID Medium die Mobiltelefon-Nr. der Person z.B. an einer Bedienstation 10 ein, und ordnet dieser Mobiltelefon-Nr. spezifische Zutrittsberechtigungen zu, im konkreten Fall wird die Berechtigung vergeben, während des vorgegebenen Nachmittags jeweils den Haupteingang des Gebäudekomplexes benützen zu dürfen.

Anschliessend werden die den Haupteingängen des Gebäudekomplexes zugeordneten eindeutigen Adressen der bei diesen Haupteingängen angeordneten Bluetooth/WLAN-Geräte 9 entweder direkt an das Mobiltelefon der Person übermittelt, normalerweise zusammen mit einer auf dem Mobiltelefon lauffähigen Software (z.B. Java), und auf diesem hinterlegt; alternativ, und diese Lösung ist insofern bevorzugt, als auf dem Mobiltelephon dadurch keine Daten gespeichert werden und somit ggf. das Mobiltelefon gewechselt werden kann, solange die gleiche Mobiltelephon Nr. zugeordnet ist, wird diese Software ohne zugeordnete Adressen der erlaubten Geräte 9 nur auf dem Zutrittskontrollsystem derart bereitgestellt, dass bei einer ersten Kontaktaufnahme des Mobiltelefons der Person (beispielsweise wenn diese sich vor der Tür befindet und eine entsprechende Mobiltelefon-Nr. zum ersten Mal wählt) mit dem Zutrittskontroll-Server respektive dessen GSM-Server 5 die zugehörige Software automatisch an das Mobiltelefon übergeben wird.

Kommt nun die Person zum richtigen Zeitpunkt, d. h. am freigegebenen Nachmittag, in die Nähe eines spezifischen Haupteingangs des Gebäudekomplexes, so empfängt das Bluetooth-fähige Mobiltelefon der Person automatisch die eindeutige Adresse des Gerätes dieses spezifischen Haupteingangs. Wurde die entsprechende Software bereits auf dem Mobiltelefon hinterlegt, erkennt nun das Mobiltelefon einen derartigen Sender. Es wird nun, ggf. automatisch, die zugehörige Software auf dem Mobiltelefon 7 ausgelöst, und, sofern erforderlich, von der Person beispielsweise aus Sicherheitsgründen zusätzlich die Eingabe eines PIN Codes abgefragt. Hat dieser den PIN Code eingegeben, so wird der Pin Code zusammen mit der eindeutigen Adresse des spezifischen Bluetooth/WLAN-Gerätes 9 des spezifischen Haupteingangs automatisch vom Mobiltelefon an das Zutrittskontrollsystem übermittelt. Dies geschieht über das GSM-Netz, entweder in Form eines SMS oder einer telephonischen Datenübermittlung, möglich ist auch ein Email oder eine andere Übermittlung nach einem bestimmten Protokoll. Im Zutrittskontrollsystem überprüft nun der Access Control-Server 4, ob dieses Mobiltelefon 7 respektive diese Mobiltelephonnummer, denn die Kennung ist nicht an das Gerät sondern an die dem Mobiltelephon zugewiesene Nummer gebunden, zu diesem Zeitpunkt an diesem (auf Grund der eindeutigen Adresse respektive auf Grund einer korrespondierenden aus dieser Adresse erzeugten Information) Durchgang berechtigt ist, und ob der eingegebene PIN Code korrekt ist. Wenn alle Bedingungen erfüllt sind, wird der Access Control-Server 4 dem zugehörigen Controller 3 derart ansteuern, dass der Schliessmechanismus 8 des Durchgangs 1 derart beeinflusst wird, dass die Person eintreten kann.

Ein weiterer Vorteil des Verfahrens ist, dass die Person ihr persönliches Mobiltelefon 7 jederzeit wechseln kann, ohne die Berechtigungen zu verlieren. Wichtig ist nur, dass die SIM Karte und somit die Telefonnummer des verwendeten Mobiltelephons die selbe bleibt. Speziell bei der Verwendung von zwei oder mehreren Mobiltelefonen 7 mit einer Mobiltelefonnummer kommt der Vorteil zu tragen. Möglich ist diese Flexibilität, weil auf dem Mobiltelefon 7 keine Daten des Zutrittskontrollsystems, höchstens die genannte Software, welche aber bei jeder Kontaktaufnahme automatisch wenn erforderlich erneut heruntergeladen wird, abgelegt sind und der Sender 9 die eindeutige Bluetooth/WLAN Adresse des Mobiltelefons 7 nicht kennen muss. In reinen auf Bluetooth basierenden

Zutrittskontrollsystemen ist dieses Problem nur sehr aufwändig lösbar.

Neben der sicheren Identifikation vor Ort ermöglicht das Verfahren auch eine Identifikation in beliebiger Distanz zum Durchgang 1, solange sich das Mobiltelefon in genügender Nähe zu einem Bluetooth/WLAN-Sender befindet, d. h. solange sich das Mobiltelefon in einem spezifischen und definierten Bereich befindet. Somit kann eine Weitbereichslösung ohne Limiten realisiert werden, die trotzdem örtlich gebunden ist. Möglich ist diese Variante insbesondere, weil der Sender 9 nicht mit dem Controller 3 verbunden sein muss und weil zudem ggf. pro Zutrittspunkt mehrere Sender 9 möglich sind. Werkszufahrten für Lieferanten sind ein solches Beispiel oder eine Remote Öffnung eines Durchganges 1 durch einen Systembediener, der keinen Zugang zu seiner Bedienstation 10 hat, aber auf dem Gelände innerhalb der Reichweite des Senders 1 ist, der diesem Durchgang 1 unter anderem zugeordnet ist. Denkbar sind beispielsweise in diesem Zusammenhang Lösungen, bei welchen Personal in einem bestimmten Arbeitsbereich, beispielsweise einem Raum mit Videokameras, welche spezifische Zugänge überwachen, und in welchem Raum sich ein Bluetooth/WLAN-Sender befindet, ermächtigt werden, mit einem Mobiltelefon einen Durchgangspunkt, welcher mit einer der Videokameras überwacht wird, zu öffnen.

BEZUGSZEICHENLISTE

1	Durchgang
2	Leser
3	Controller
4	Access Control-Server
5	GSM-Server
6	Antenne (schematisch)
7	Mobiltelefon
8	physikalischer Schliessmechanismus (Schloss)
9	Bluetooth-Sender
10	Bedienstation

PATENTANSPRÜCHE

1. Zutrittskontrollsystem mit

- einem Standard-Zutrittskontrollsystem (2-4,8), über welches eine Vielzahl von Zutrittspunkten (1) über jeweils individuelle physikalische Schliessmechanismen (8) kontrolliert werden können, wobei bei jedem Zutrittspunkt (1) wenigstens ein Leser (2) sowie ein damit in Verbindung stehender Controller (3) zur Steuerung des Schliessmechanismus' (8) vorgesehen ist, und wobei wenigstens ein Access Control-Server (4) vorhanden ist, welcher eine zentrale Verwaltung der Zutrittsdaten vornimmt, und welcher mit den jeweiligen Controllern (3) in Verbindung steht;

- wenigstens einem Mobiltelefonie-Server (5) in Verbindung mit dem Access Control-Server (4), welcher wenigstens indirekt in der Lage ist, Daten über ein Mobiltelefon-Netz an Mobiltelefon-Teilnehmer (7) abzusetzen respektive von diesen zu empfangen, wobei dieser Mobiltelefonie-Server (5) auch integraler Bestandteil des Access Control-Server (4) sein kann;

dadurch gekennzeichnet, dass

an einem spezifizierten Ort ein kurzreichweitiger Sender (9) vorhanden ist, welcher Zutrittspunkt-spezifische Identifikationsinformation derart aussendet, dass sie von einem in Empfangsnähe des Senders (9) befindlichen Mobiltelefon (7) empfangen und von diesem wenigstens indirekt zur Steuerung der Zutrittskontrolle eines spezifischen zugeordneten Zutrittspunkts (1) verwendet wird.

2. Zutrittskontrollsystem nach Anspruch 1, dadurch gekennzeichnet, dass es sich beim spezifizierten Ort um einen Ort im Bereich des zugeordneten Zutrittspunkts (1) handelt, so dass die Identifikationsinformation des Senders (9) nur in unmittelbarer Nähe des Zutrittspunkts (1) vom Mobiltelefon (7) empfangen werden kann.

3. Zutrittskontrollsystem nach Anspruch 1, dadurch gekennzeichnet, dass es sich beim spezifizierten Ort um einen dem zugeordneten Zutrittspunkt (1) vorgelagerten Ort oder um einen spezifischen Arbeitsbereich handelt.

4. Zutrittskontrollsystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass es sich beim Sender (9) um ein Bluetooth-Gerät, insbesondere bevorzugt mit einer Reichweite von weniger als 10 Metern, handelt, und dass das berechtigte Mobiltelefon (7) über eine Bluetooth-Schnittstelle verfügt.

5. Zutrittskontrollsystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass es sich beim Sender (9) um eine WLAN-Station handelt, und dass das berechtigte Mobiltelefon (7) über eine WLAN-Schnittstelle verfügt.

6. Zutrittskontrollsystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass es sich bei der Identifikationsinformation um eine Hardware-spezifische, eindeutige Adresse des Senders (9), insbesondere bevorzugt um eine gerätespezifische 48-bit-Adresse eines Bluetooth-Geräts (9) respektive eine entsprechende Gerät spezifische Adresse eines WLAN-Gerätes respektive eines WLAN-Netzes handelt.

7. Zutrittskontrollsystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Sender (9) als unabhängige Einheit ausgebildet ist, welche bevorzugt über keine direkte Verbindung mit dem Standard-Zutrittskontrollsystem (2-4,8) und/oder dem Mobiltelefonie-Server (5) verfügt.

8. Zutrittskontrollsystem nach einem der vorhergehenden Ansprüche, dadurch

gekennzeichnet, dass das Standard Zutrittskontrollsystem (2-4,8) zudem die Zutrittskontrolle unter Verwendung von Mitteln ohne Mobiltelefonie (7) erlaubt, insbesondere auf Basis von RFID-Technologie.

9. Verfahren zur Zutrittskontrolle, insbesondere bevorzugt unter Verwendung eines Zutrittskontrollsystems nach einem der vorhergehenden Ansprüche, wobei

ein Standard-Zutrittskontrollsystem (2-4,8), über welches eine Vielzahl von Zutrittspunkten (1) über jeweils individuelle physikalische Schliessmechanismen (8) kontrolliert werden können, vorhanden ist, wobei bei jedem Zutrittspunkt (1) bevorzugt wenigstens ein Leser (2) sowie ein damit in Verbindung stehender Controller (3) zur Steuerung des Schliessmechanismus' (8) vorgesehen ist, und wobei wenigstens ein Access Control-Server (4) vorhanden ist, welcher eine zentrale Verwaltung der Zutrittsdaten vornimmt, und welcher mit den jeweiligen Controllern (3) in Verbindung steht;

und wobei wenigstens ein Mobiltelefonie-Server (5) in Verbindung mit dem Access Control-Server (4) vorhanden ist, welcher wenigstens indirekt in der Lage ist, Daten über ein Mobiltelefon-Netz an Mobiltelefon-Teilnehmer (7) abzusetzen respektive von diesen zu empfangen, wobei dieser Mobiltelefonie-Server (5) auch integraler Bestandteil des Access Control-Servers (4) sein kann;

dadurch gekennzeichnet, dass

an einem spezifizierten Ort, bevorzugt bei wenigstens einem Zutrittspunkt (1), ein kurzreichweitiger Sender (9) vorhanden ist, dass

ein Mobiltelefon (7) zum Zutritt bestimmter Zutrittspunkte (1) in einem bestimmten Zeitraum über den Access Control-Server (4) respektive über den Mobiltelefonie-Server (5) über das Mobiltelefon-Netz autorisiert wird,

dass der Sender (9) Zutrittspunkt-spezifische Identifikationsinformation kontinuierlich oder abschnittsweise derart aussendet, dass sie von einem nur in Empfangsnähe des Senders befindlichen Mobiltelefon (7) empfangen werden kann,

dass ein in Empfangsnähe des Senders (9) befindliches Mobiltelefon (7) die Kennung dieses Senders (9)über diese Identifikationsinformation erfasst,

und dass anschliessend über Mobiltelefon (7), Mobiltelefon-Netz, Mobiltelefonie-Server (5), Access Control-Server (4), respektive Controller (3) die Öffnung des dem Sender (9) zugeordneten Zutrittspunktes (1) unter direkter oder indirekter Verwendung dieser Identifikationsinformation veranlasst wird.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass der Sender (9) derart in der Nähe des Zutrittspunkts (1) angeordnet ist, dass das Mobiltelefon (7) dessen Identifikationsinformation nur in unmittelbarer Nähe des Zutrittspunkts (1) empfangen kann.

11. Verfahren nach einem der Ansprüche 9 oder 10, dadurch gekennzeichnet, dass das Mobiltelefon (7) nach Erfassung der Identifikationsinformation zusätzlich die Eingabe einer Authentifikation wie insbesondere eines PIN-Codes, Passworts oder biometrischer Information (7) verlangt, und diese benutzerspezifische Information zusammen mit der Kennung des zu bearbeitenden Zutrittspunkts (1) über das Mobiltelefon-Netz an den Mobiltelefonie-Server (5) und den Access Control-Server (4) übergeben wird, und dieser anschliessend den zugehörigen Controller (3) aktiviert.

12. Verfahren nach einem der Ansprüche 9-11, dadurch gekennzeichnet, dass das Mobiltelefon (7) die Identifikationsinformation und gegebenenfalls den PIN-Code über das GSM-Netz in Form einer telefonischen Datenübermittlung oder in Form eines SMS an den Access Control-Server (4) übergibt.

13. Verfahren nach einem der Ansprüche 7 oder 8, dadurch gekennzeichnet, dass es sich beim Sender (9) um ein Bluetooth- oder ein WLAN-Gerät (9) handelt,

welches als Identifikationsinformation seine eindeutige Adresse aussendet, und diese Adresse zur Kennung des zugehörigen Zutrittspunkts (1) dient, und dass das Mobiltelefon (7) über eine Bluetooth-respektive über eine WLAN-Schnittstelle verfügt, wobei das Mobiltelefon (7) bei Empfangen spezifischer, im Rahmen der Autorisierung übertragener derartiger Adressen, welche den autorisierten Zutrittspunkten (1) entsprechen, automatisch in einen entsprechenden Dialog mit dem Mobiltelefon-Benutzer eintritt, gegebenenfalls eine Authentifikation des Benutzers anfordert, und auf jeden Fall anschliessend eine Öffnungsanfrage des spezifischen Zutrittspunkts (1) über das Mobiltelefon-Netz an den Mobiltelefonie-Server (5) respektive den Access Control-Server (4) übermittelt wird.

14. Verfahren nach einem der Ansprüche 9-13, dadurch gekennzeichnet, dass es sich beim Sender (9) um ein Bluetooth- oder ein WLAN-Gerät (9) handelt, welches derart im Bereich des Durchgangs (1) angeordnet ist, dass der Empfang der Identifikationsinformation durch ein Mobiltelefon (7) nur in einem Abstand von weniger als 1m, bevorzugt weniger als 0.5m ausserhalb und vor dem Durchgang (1) möglich ist.

15. Verfahren nach einem der Ansprüche 9-14, dadurch gekennzeichnet, dass es sich beim Sender (9) um ein Bluetooth- oder ein WLAN-Gerät (9) handelt, welches in einem dem zugeordneten Zutrittspunkt (1) vorgelagerten spezifischen Bereich oder in einem dem Zutrittspunkt zugeordneten Arbeitsbereich angeordnet ist.

16. Zeiterfassungssystem mit

- einem Standard-Zeiterfassungssystem, welches wenigstens einen Zeiterfassungs-Server (4) umfasst, welcher eine zentrale Verwaltung der Zeitdaten vornimmt;

- wenigstens einem Mobiltelefonie-Server (5) in Verbindung mit dem

Zeiterfassungs-Server (4), welcher wenigstens indirekt in der Lage ist, Daten über ein Mobiltelefon-Netz an Mobiltelefon-Teilnehmer (7) abzusetzen respektive von diesen zu empfangen, wobei dieser Mobiltelefonie-Server (5) auch integraler Bestandteil des Zeiterfassungs-Servers (4) sein kann;

dadurch gekennzeichnet, dass

bei wenigstens einem autorisierten Bereich (1) ein kurzreichweitiger Sender (9) vorhanden ist, welcher Bereichs-spezifische Identifikationsinformation derart aussendet, dass sie von einem nur in unmittelbarer Nähe des autorisierten Bereichs (1) befindlichen Mobiltelefon (7) empfangen und von diesem wenigstens indirekt zur Manipulation der Zeitdaten verwendet wird.

17. Verfahren zur Zeiterfassung, insbesondere bevorzugt unter Verwendung eines Zeiterfassungssystems nach Anspruch 12, wobei

ein Standard-Zeiterfassungssystem, welches wenigstens einen Zeiterfassungs-Server (4) umfasst, welcher eine zentrale Verwaltung der Zeitdaten vornimmt;

und wobei wenigstens ein Mobiltelefonie-Server (5) in Verbindung mit dem Zeiterfassungs-Server (4) vorhanden ist, welcher wenigstens indirekt in der Lage ist, Daten über ein Mobiltelefon-Netz an Mobiltelefon-Teilnehmer (7) abzusetzen respektive von diesen zu empfangen, wobei dieser Mobiltelefonie-Server (5) auch integraler Bestandteil des Zeiterfassungs-Servers (4) sein kann;

dass bei wenigstens einem autorisierten Bereich (1) ein kurzreichweitiger Sender (9) vorhanden ist,

dadurch gekennzeichnet, dass

ein Mobiltelefon (7) zur Eingabe von Zeitdaten in bestimmten autorisierten Bereichen (1) in wenigstens einem bestimmten Zeitraum über den Zeiterfassungs-Server (4) respektive über den Mobiltelefonie-Server (5) über das Mobiltelefon-Netz autorisiert wird,

dass der Sender (9) Bereichs-spezifische Identifikationsinformation

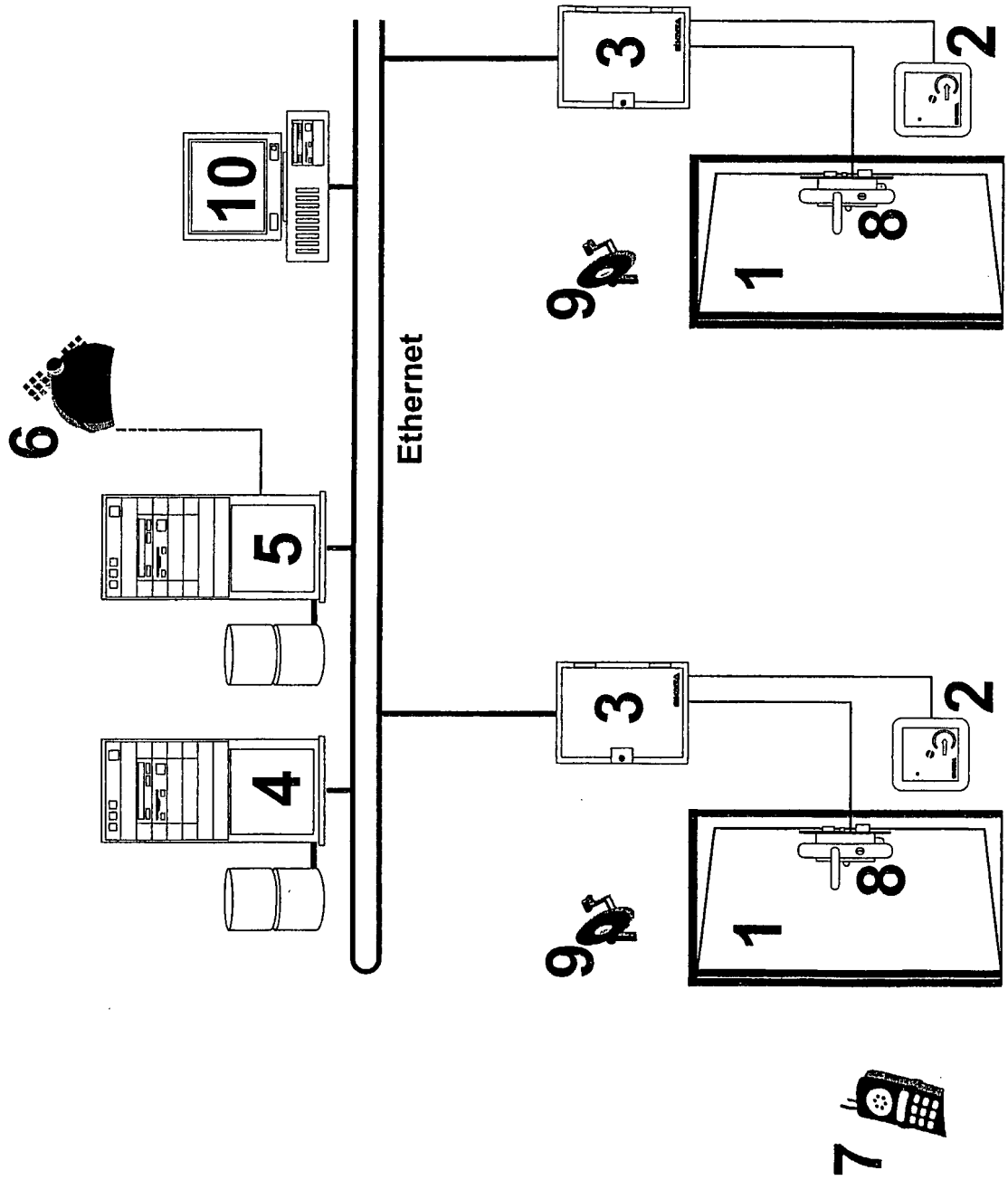
kontinuierlich oder abschnittsweise derart aussendet, dass sie von einem nur in unmittelbarer Nähe des autorisierten Bereichs (1) befindlichen Mobiltelefon (7) empfangen werden kann,

dass ein in unmittelbarer Nähe des Bereichs (1) befindliches Mobiltelefon (7) die Kennung dieses Bereichs (1) über diese Identifikationsinformation erfasst,

und dass anschliessend über Mobiltelefon (7), Mobiltelefon-Netz, Mobiltelefonie-Server (5) Zeitdaten an den Zeiterfassungs-Server (4) übermittelt, respektive von diesem abgefragt werden.

18. Auf einem Mobiltelefon (7) lauffähiges Datenverarbeitungsprogramm zur Durchführung eines Verfahrens nach einem der Ansprüche 9-15, welches dazu ausgelegt ist, die über eine Bluetooth- oder WLAN-Schnittstelle empfangene Identifikationsinformation eines Senders (9), gegebenenfalls zusammen mit einer in einer Abfrage angeforderten zusätzliche Information wie beispielsweise einem PIN-Code, einem Passwort oder biometrischer Information, in automatisierter Art über das GSM-Netz an einen Access Control-Server (4) zu übermitteln.

19. Mobiltelephon (7) mit einem Datenverarbeitungsprogramm nach Anspruch 18.


Ethernet
1
2
3
4
5
6
7
8
9
10